МЕТОДЫ И ТЕХНОЛОГИИ ПРИНЯТИЯ РЕШЕНИЙ

УДК 004.3 *Научная статья* DOI: 10.18287/2223-9537-2023-13-1-125-138

Многоаспектное моделирование ситуаций в задачах обеспечения функциональной безопасности аппаратно-программных комплексов

© 2023, В.Е. Гвоздев, О.Я Бежаева ✉, Г.Р. Сафина

Уфимский университет науки и технологий, Уфа, Россия

Аннотация

Функциональная безопасность является латентной характеристикой аппаратно-программных комплексов (АПК) и объективно характеризуется удовлетворённостью потребителей поведением АПК. В работе рассматривается подход к решению задач, связанных с управлением проектом, на основе анализа динамических характеристик функциональной безопасности конфликтных ситуаций в системе управления проектом. Для анализа ситуаций, возникающих при управлении проектами создания АПК возможно использование моделей, известных как системные архетипы. Рассмотрены информационная сущность ситуаций и основы многоаспектного моделирования. Методическую основу исследований составляет сочетание динамических моделей параметров, характеризующих функциональную безопасность, и структурных моделей, соответствующих конфликтным ситуациям, возникающим при обеспечении требуемого уровня функциональной безопасности. Рассмотрены примеры многоаспектного моделирования ситуаций, где в качестве событий выступают проявления латентных дефектов. В результате исследований: определены информационные сущности ситуаций, предложены концептуальные основы многоаспектного моделирования ситуаций, возникающих при управлении функциональной безопасностью АПК, выделены базовые этапы построения системы структурных и динамических моделей ситуаций на разных стадиях жизненного цикла АПК. Полученные результаты могут быть использованы для принятия решений о целесообразности внесения изменений в структуру системы обеспечения функциональной безопасности АПК.

Ключевые слова: *функциональная безопасность, аппаратно-программный комплекс, сетецентрическое управление, системный архетип, структурные модели.*

Цитирование: *Гвоздев В.Е., Бежаева О.Я., Сафина Г.Р.* Многоаспектное моделирование ситуаций в задачах обеспечения функциональной безопасности аппаратно-программных комплексов // Онтология проектирования. 2023. Т.13, №1(47). С.125-138. DOI: 10.18287/2223-9537-2023-13-1-125-138.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Введение

Возрастание роли систем обработки данных в управлении распределёнными техническими системами выдвигает на первый план обеспечение функциональной безопасности (ФБ) аппаратно-программных комплексов (АПК). Цифровая экосреда является системообразующим фактором сетецентрического управления территориально распределёнными сложными техническими системами (СТС). Базовым требованием к их информационной инфраструктуре является предоставление своевременной полной и достоверной информации, необходимой для урегулирования ситуаций, возникающих в разных частях распределённой

СТС. Потребительские свойства АПК определяется качеством управления проектами создания АПК [1], относящихся к классу субъектоцентрических систем [2].

Безопасность является латентной характеристикой АПК и объективно характеризуется удовлетворённостью потребителей поведением комплекса. В настоящей работе рассматривается подход к решению задачи, связанной с управлением проектом АПК и состоящей в выявлении конфликтных ситуаций, имеющих место в системе управления проектом.

1 Подходы к обеспечению ФБ АПК

При создании АПК обеспечение безопасного их функционирования является важнейшей задачей [3, 4]. В [1, 3] отмечается необходимость развития методологических и теоретических основ дефектологии АПК как одного из направлений исследований в области системной инженерии. В [4] выделяются классы задач, связанные с обеспечением технологической и эксплуатационной безопасности. В [5, 6] отмечается необходимость совершенствования систем управления проектами создания компонент распределённых коммуникационно-вычислительных систем. В [3, 7, 8] выделяются задачи, связанные с обеспечением конфиденциальности, целостности и доступности информации в случае, когда пользователи принимают активное участие в управлении СТС. Задачи, связанные с обеспечением ФБ АПК при решении задач управления в реальном времени, обсуждаются в [9, 10].

Под ФБ АПК понимается свойство сохранять работоспособность в соответствии с целевым назначением при случайных дестабилизирующих воздействиях и отсутствии злоумышленного влияния на программную, аппаратную составляющие и базы данных [3]. Из анализа работ [11-13] можно сделать заключение о том, что ФБ определяется не выявленными (латентными) дефектами в конструкции АПК. Дефекты являются следствием ошибок, допускаемых разработчиками АПК на разных стадиях их жизненного цикла (ЖЦ). Существуют разные подходы к управлению непреднамеренно допускаемыми дефектами на разных стадиях ЖЦ, включая предпроектную стадию. Важное значение имеет природа возникновения дефектов. На начальных стадиях ЖЦ преобладают дефекты, обусловленные неопределённостью среды использования и нечёткостью целей управления. По мере перехода от начальных стадий ЖЦ к последующим акценты перемещаются в области: неверного использования руководств по разработке; технологий использования инструментальных средств; нарушения условий применимости моделей ЖЦ АПК. Используемые методы управления дефектами можно соотнести с проактивным, активным и реактивным подходами к управлению СТС.

К настоящему времени развитие получили методы, соотносимые с активным и реактивным подходами, т.е. ориентированные на выявление ошибок по результатам специально организованных испытаний и изучения исторических данных об опыте эксплуатации АПК с целью установления закономерностей в проявлениях симптомов дефектов, а также причин возникновения дефектов. Эту группу методов, можно объединить понятием - анализ коренных причин отказов [14]. Они являются адаптацией положений теории решения изобретательских задач [15] в область управления ФБ АПК, а именно методов, относящихся к диверсионному анализу [16]. К другому развиваемому в настоящее время направлению активного подхода к обеспечению ФБ АПК относятся методы, которые можно объединить понятием анализ распространения ошибок [17-19]. Суть этих методов состоит в раннем обнаружении проявлений дефектов и сбоев и парировании этих явлений. К методам, основу которых составляет проактивный подход к управлению СТС, следует отнести методы, ориентированные на сравнительный анализ альтернатив проектных решений по критериям ФБ (анализ видов и последствий отказов; анализ дерева отказов) [20-22].

В работах [23, 24] к числу критических факторов, негативно влияющих на успех реализации проектов создания АПК, относятся функциональные[1] и нефункциональные требования[2] к потребительским свойствам систем. Это обусловлено сложностью формирования консолидированного мнения различных целевых групп пользователей в условиях неопределённости среды использования и размытости целей функционирования СТС [2, 25-27]. В работах [26, 27] обосновывается необходимость развития подходов к выработке консолидированных решений на основе методов конвергентного управления и развития сетевых технологий согласования решений заинтересованных сторон.

2 Информационная сущность ситуаций

Информационная сущность ситуаций, связанных с обеспечением ФБ АПК, формируется на основе следующих понятий.

События - проявление взаимодействий процессов, протекающих как внутри исследуемого объекта, так и вне его. Событие объективно. Ситуация определяется местом субъекта внутри события, его озабоченностью событием. Степень озабоченности влияет на восприятие события субъектом, составляет основу для выделения симптомов ситуаций, формирования описания ситуации [2, 25]. Описание ситуации служит основанием получения ответа на вопросы: в чём содержание события и как наилучшим образом реагировать на событие сейчас? Режим понимания ситуаций – реактивный.

Шаблоны событий предназначены для выявления наиболее вероятных условий возникновения событий, которые неоднократно имели место ранее. Режим понимания – адаптивный, что определяет выбор способов наиболее эффективного реагирования на события. Составляющая, связанная с управлением ситуацией, т.е. стимулированием возникновения /предотвращением возникновения событий, в шаблонах отсутствует.

Систематическая структура предназначена для выявления «генераторов», «виновников» возникновения событий. При формировании систематических структур необходимо определить системообразующие факторы (в том числе гипотетические, ранее не наблюдавшиеся). Установление причин возникновения ситуаций есть производная от ментальных моделей исследователей, основу которых составляют представления о ценностях. Режим понимания – креативный, определяемый ментальными моделями субъектов - конструкторов систематических структур. Выявление условий возникновения ситуаций создаёт базу для влияния на них, т.е. выбора «точек приложения рычага» [28] изменения ситуаций в нужную сторону.

Расширенное видение - понимание того, что хочется получить в результате урегулирования ситуации, какие альтернативы систематических структур позволят достичь желаемого. Новые знания изменяют положение дел как за счёт инженерных решений, так и за счёт изменения ментальных моделей с учётом понимания сложности событий и ограниченности ресурсов для урегулирования ситуаций. Это соответствует генеративному режиму понимания событий.

Информационная сущность делает возможным построение разных знаковых моделей характеристик ФБ, которые создают основу для выработки обоснованных решений по урегули-

[1] Функциональные требования описывают сервисы, предоставляемые АПК или программной системой, её поведение в определённых ситуациях, реакцию на входные данные и действия, которые система позволит выполнить пользователям.

[2] Нефункциональные требования фиксируют условия, которые непосредственно не связаны с поведением или функциональностью решения, а скорее описывают условия окружающей среды, при которых решение должно оставаться эффективным, или качества, которыми система должны обладать. Они также известны как атрибуты (показатели) качества или дополнительные требования. Они могут включать требования, связанные с пропускной способностью, надёжностью, масштабируемостью, скоростью, безопасностью, доступностью, информационной архитектурой и др.

рованию ситуаций. Одной из разновидностей структурных моделей ситуаций являются так называемые «системные архетипы» (СА) [29].

СА составляют основу решения двух классов задач: диагностических и прогностических. Основой решения диагностических задач является выбор из доступного множества СА того, который соответствует наблюдаемым симптомам ситуации. Это позволяет на качественном уровне определить основные причины сложившейся ситуации и подходы к её урегулированию. Рекомендации по урегулированию ситуаций, соответствующих разным СА, приведены в [29]. Одной из разновидностей прогностических задач является выявление по результатам анализа динамических характеристик поведения СТС конфликтных ситуаций в системе управления. Результатом решения задачи является параметрическая настройка существующей структуры системы управления либо внесение изменения в структуру. Получаемые оценки зависят от динамических характеристик поведения, учитываемых при выявлении ситуаций. Полученные результаты создают основу планирования системы мер по целенаправленному изменению структуры и параметров системы управления («выбора точки приложения рычага» [30]).

3 Концептуальная основа многоаспектного моделирования

Концептуальную основу моделирования СТС составляют следующие положения.

- АПК есть разновидность СТС. Это даёт основание научной адаптации моделей ситуаций, возникающих при управлении СТС иной природы, в область управления ФБ АПК.
- Признаком наличия ситуаций являются симптомы событий, которые характеризуют отклонение поведения системы от ожидаемого. Различные субъекты (аналитики, постановщики задач, проектировщики, испытатели, системные администраторы, пользователи и потребители информационных продуктов и услуг), вовлечённые в урегулирование ситуаций, в силу различия их ментальных моделей по-разному воспринимают одно и то же событие и по-разному выделяют ситуации. Последнее обстоятельство служит причиной одновременного использования разных моделей ситуаций для характеристики одного и того же события.
- Соответствие свойств системы запросам потребителей определяется качеством управления на всех стадиях ЖЦ АПК: от обследования информационных потребностей, желаний и представлений о ценностях потребителей, до эксплуатации и модернизации АПК. Свойства АПК определяются их устройством и проявляются как внешнее поведение. Ошибки в организации управления проектом представляют наибольшую опасность для результатов проекта.
- Особенностью СТС является наличие множества взаимодействующих контуров причинно-следственных связей параметров, определяющих поведение системы, а также задержек времени между оказываемыми на систему воздействиями и последствиями от их проявления. Особенности взаимодействия контуров изменяются во времени.

Известные рекомендации по урегулированию ситуаций на основе выделения СА носят качественный характер [29]. Недостаточное развитие получили структурные и математические модели, посредством которых можно обеспечить информационную поддержку выбора обоснованного подхода к урегулированию ситуаций. В настоящей статье методическую основу исследований составляет системное сочетание динамических моделей параметров, характеризующих ФБ, и структурных моделей, соответствующих конфликтным ситуациям, возникающим при обеспечении требуемого уровня ФБ.

4 Этапы построения моделей ситуаций

Основными этапами построения системы структурных и динамических моделей ситуаций в рамках архитектурного подхода, содержание которого представлено в стандарте *IEEE* 1471[3], являются следующие.

- *Определение подхода к исследованиям*. Множественность точек зрения на события, влияющих на поведение показателей ФБ АПК, является проявлением свойства полиморфизма моделей. Точка зрения на событие предопределяет выбор существенных факторов, т.е. подходы к построению моделей и границы их применимости.
- *Временной горизонт.* Наличие адекватных структурных моделей ситуаций и динамических моделей изменения поведения ситуации во времени делает возможным оценить временные горизонты, в которых целесообразно обсуждать подходы к урегулированию ситуации.
- *Определение границ описания ситуации*. Этап предопределяет выделение минимально достаточного множества характеристических параметров ситуации.
- *Определение уровня детальности описания ситуации* (уровня абстракции): определяется уровнем понимания содержания ситуации, также временным горизонтом, в пределах которого предполагается урегулирование ситуации. Целью построения системы моделей является обобщение частных динамических характеристик к виду СА.
- *Значимые задержки*. Построение на основе анализа частных динамических характеристик СА создаёт основу для выделения значимых задержек в системе обеспечения ФБ. Задержки являются причиной нарастающего дисбаланса между свойствами разных частей системы. Своевременно выявленные временные задержки могут сыграть роль предохранительного клапана, препятствующего преобразованию дисбаланса в негативные последствия. Недостаточный учёт роли временных задержек может явиться причиной взрывного изменения свойств системы.

5 Примеры многоаспектного анализа ситуаций

В качестве событий в примерах многоаспектного анализа ситуации, связанных с обеспечением ФБ программной компоненты АПК, выступают проявления латентных дефектов, негативно влияющих на возможность получения ценных для потребителя информационных продуктов и услуг.

Пример 1. Влияние устранения латентных дефектов на показатели ФБ.

Описание задачи. Показателем ФБ является вероятность успешного завершения/отказа программы в серии прогонов. Считается, что при реализации серии сведения о проявлениях дефектов, их местоположении и характере лишь собираются. После завершения серии прогонов выполняется анализ коренных причин отказов, и в ПС вносятся изменения, улучшающие её свойства.

Требуется: построить совокупность моделей, способствующих повышению обоснованности принятия решения относительно объёмов ресурсов, необходимых для обеспечения требуемого уровня показателя ФБ.

Описанной задаче можно сопоставить структурную модель, представленную на рисунке 1.

Здесь:

[3] Стандарт IEEE 1471-2000 - рекомендуемая практика описания архитектуры систем, интенсивно использующих программное обеспечение (*Recommended Practice for Architectural Description of Software — Intensive Systems*). https://standards.ieee.org/ieee/1471/2187/.

S_1 – этап подготовки исходных данных, соответствующих запросам пользователей;
S_2 – этап оформления информационных продуктов и сервисов и передачи их потребителям;
S_3 – состояние системы, при котором с вероятностью P дефекты проявляются;
S_4 – состояние системы, при котором дефекты не проявляются с вероятностью $Q = 1-P$;

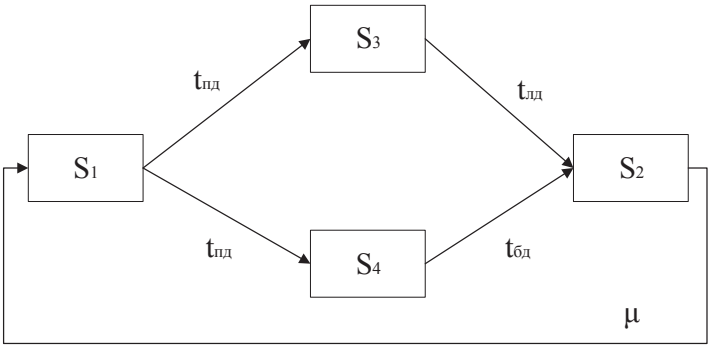

Рисунок 1 - Структурная модель точки зрения на ситуацию

$t_{пд}$ – время подготовки данных, соответствующих запросам потребителей;
$t_{лд}$ – время устранения проявившихся дефектов и последующей обработки данных;
$t_{бд}$ – время обработки данных в случае, когда латентные дефекты не проявляются;
μ – интенсивность запросов пользователей.

Имитационный эксперимент выполнен по следующему укрупнённому алгоритму.

Шаг 1. Задаётся ограничение на время обработки запроса пользователей $T_{гр}$. Если время обработки запроса превышает это значение, считается, что произошел отказ ПС [31].

Шаг 2. Посредством датчиков случайных чисел генерируются значения времени подготовки данных $t_{пд}^{(i)}$; время устранения проявившихся дефектов и последующей обработки данных $t_{лд}^{(i)}$**,** время обработки данных в случае, когда латентные дефекты не проявляются $t_{бд}^{(i)}$**.** Время между поступлениями заданий (на вход блока S_1) генерировалось посредством датчика случайных чисел на основании μ. В качестве распределения случайных величин принимался показательный закон. Его выбор обоснован тем, что он является характеристикой простейшего потока событий [32]. При этом параметры закона принимались обратными математическим ожиданиям $M[t_{пд}]$,$M[t_{лд}]$ и $M[t_{бд}]$. В ходе проведения исследований принималось, что $M[t_{пд}] < M[t_{лд}]$. Чтобы обеспечить устойчивость статистических оценок, число реализаций в серии принималось равным 1000.

Шаг 3. Выбор пути обработки данных (по ветке P либо ветке Q) для каждой заявки, поступающей на вход блока S_1, осуществлялся случайным образом. Путь, на котором дефект проявлялся, выбирался с вероятностью P, а путь, на котором дефект не проявлялся, - с вероятностью Q. Для каждой i-й заявки генерировались $t_{пд}^{(i)}$ (когда выбиралась ветка Q), либо $t_{лд}^{(i)}$ (когда выбиралась ветка P). Общее время обработки заявки $T_{общ}^{(i)}$ определялось как сумма времён подготовки и обработки данных. При этом в качестве времени обработки данных выбиралось $t_{лд}^{(i)}$ (когда выбиралась ветка P), либо $t_{пд}^{(i)}$ (когда выбиралась ветка Q). Если соблюдалось условие $T_{общ}^{(i)} < T_{гр}$, считалось, что заявка обслужена успешно. В противном случае считалось, что произошел отказ ПС.

Шаг 4. На основе массива данных о результатах испытаний серии оценивалась вероятность отказа /безотказной работы ПС.

Шаг 5. Выполнялась оценка влияния усилий на выявление и устранение латентных дефектов на показатели ФБ. Для этого вносились изменения в значения вероятности проявления латентных дефектов при прогоне ПС по правилу*:* $P_l = P_{l-k}/l$**.** Здесь l- номер серии испытаний; k - задержка времени (выражаемая количеством серий) между внесением улучшений и проявлением последствий этого.

На рисунке 2 представлены динамические характеристики интегрального показателя ФБ - вероятности отказа $P_{отк}$ АПК при разных значениях временной задержки $\boldsymbol{k}$.

Полученные зависимости создают основу планирования ресурсов (затрат времени на уменьшение вероятности проявления латентных дефектов) для обеспечения требуемых значений показателя ФБ. Выделенной ситуации ставится в соответствие СА «Уравновешивание с задержкой» (рисунок 3):

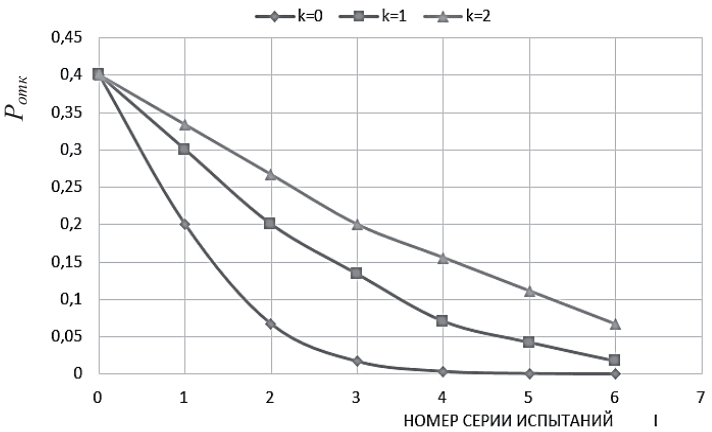

Рисунок 2 - Динамические характеристики интегрального показателя ФБ

Контурная модель, представленная на рисунке 3, представляет собой стабилизирующий цикл. Характеристикой состояния ПС является вероятность безотказной работы/отказа.

На рисунке 4 представлен демонстрационный пример изменения вероятности отказа ПС в случае, когда усилия, направленные на уменьшение вероятности проявления латентных дефектов, не предпринимаются.

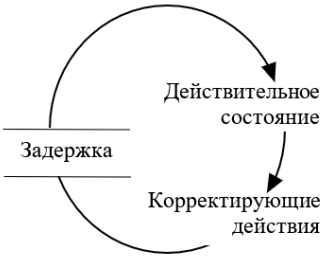

Рисунок 3 - СА «Уравновешивание с задержкой»

Пример 2. Эффективность использования ресурсов на устранение дефектов.

Описание задачи. Обеспечение ФБ реализуется на основе реактивного и проактивного подходов. В реактивном подходе осуществляется выявление и устранение проявившихся дефектов; проактивного – создание барьеров, препятствующих возникновению дефектов. При планировании проектов следует принимать обоснованные решения по выделению ресурсов на реализацию разных видов деятельности, как в рамках реактивного, так и проактивного подходов. Одним из критериев принятия решений является анализ динамики эффективности устранения дефектов.

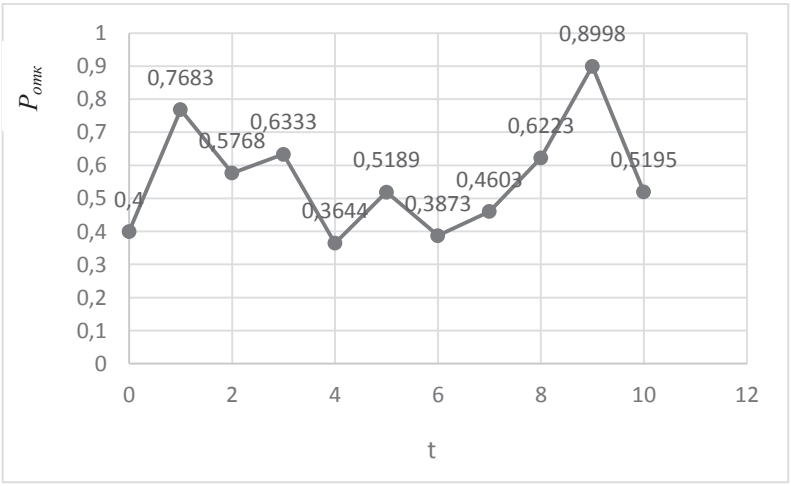

Рисунок 4 - Демонстрационный пример изменения вероятности отказа АПК при отсутствии подхода к уменьшению вероятности проявления латентных дефектов

Объективными косвенными показателями ФБ являются латентные дефекты [33]. Объективным показателем изменения ФБ является динамика количества выявленных дефектов в результате целенаправленной деятельности по выявлению и устранению латентных дефектов [1]. В силу свойства уникальности проектов [34] и субъектоцентрического характера программных проектов, модели динамики количества выявленных дефектов целесообразно строить в классе эмпирических моделей [35]. Модели, позволяющие оценить количество невыявленных дефектов, описаны, например, в [33].

Постановка задачи. Дано: динамика относительного показателя *D(t),* характеризующего выявленные дефекты (например, в виде количества дефектов на 1000 строк кода); динамика затрат ресурсов на выявление дефектов *S(t)*; критерий эффективности устранения дефектов вида *E(t)=D(t)/S(t)*; нижняя граница критерия эффективности *E*,* меньше которой дальнейшие затраты ресурсов на устранение дефектов становятся нецелесообразными.

Требуется: построить зависимость *E(t)* и определить границу ресурсов (времени) t*, соответствующую *E**.

Допущения: постулируется, что зависимость *D(t)* имеет вид:

$$D(t) = K*exp(-\Lambda*t), \quad (1)$$

где *K* - исходное значение относительного показателя засоренности дефектами. Возможные подходы к оцениванию *K* описаны, например, в [33].

Зависимость затрат на устранение дефектов имеет вид:

$$S(t) = exp(\mu*t)-1 \quad (2)$$

Пример решения задачи выполнен при значении Λ и μ равных единице; *K*=0.4. На рисунке 5 представлены зависимости *D(t)* и *S(t).*

Временные отметки τ_i *(i=1, 2, 3,…)* соответствуют значениям $D(t) = D(0)/(2)^{(i)}$, т.е. это отметки времени, в которых количество дефектов по сравнению с предыдущей отметкой уменьшилось вдвое.

В таблице 1 приведены значения *D(t), S(t), E(t),* соответствующие разным отметкам времени τ_i. На рисунке 6 приведена графическая модель, характеризующая поведение *E(t)* и построенная на основе данных, представленных в таблице 1.

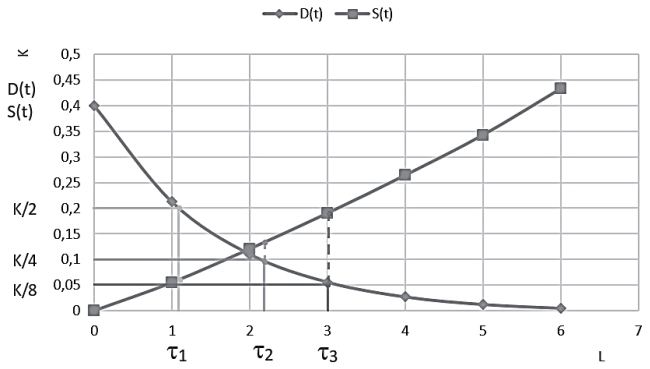

Рисунок 5 - Динамические модели *D(t)* и *S(t)*

Таблица 1 – Значения $D(\tau_i)$, $S(\tau_i)$, $E(\tau_i)$ соответствующие разным отметкам времени τ_i.

i	τ_i	$D(\tau_i)$	$S(\tau_i)$	$E(\tau_i)$
1	1,1	0,20	0,07	3,43
2	2,2	0,10	0,14	0,87
3	3,0	0,05	2,00	0,28
4	4,0	0,02	2,26	0,10

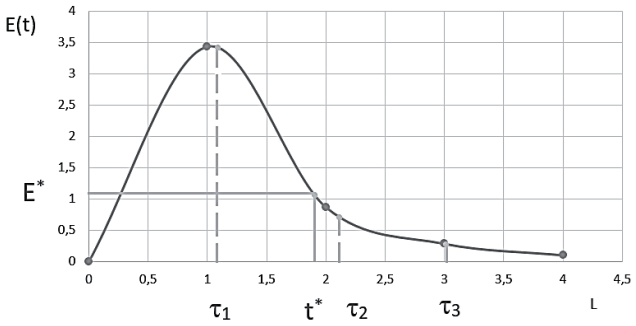

Рисунок 6 - Характеристика эффективности устранения дефектов

Зависимость *E(t)* построена при условии, что *E(0)*=0, так как если усилий по устранению дефектов не прилагается, эффект отсутствует.

На основе зависимости *E(t)* (рисунок 6) при заданном *E** можно оценить границы периода (ресурс времени) $T \in [0; t^*)$, в течение которого имеет смысл совершенствовать ФБ за счёт выявления и устранения дефектов.

Выделенному видению задач обеспечения ФБ АПК можно поставить в соответствие СА «Пределы роста» (рисунок 7).

Рисунок 7 - Структурная модель, соответствующая СА «Пределы роста»

С течение времени действия по устранению дефектов приводят к уменьшению их количества (усиливающий контур ФБ). Вместе с тем, с течением времени стоимость устранения дефектов возрастает. Это препятствует выделению ресурсов на другие виды деятельности, связанные с обеспечением ФБ, например, за счёт создания и совершенствования барьеров, препятствующих возникновению дефектов на разных стадиях ЖЦ АПК.

Пример 3. Анализ сбалансированности параметров проекта

Описание задачи. Уровень потребительских свойств программных продуктов, включая ФБ, определяется подходами к решению комплекса задач, связанных с реализаций программных проектов [36]. Основа успешности программного проекта – сбалансированность требований к потребительским свойствам предполагаемого продукта и объёмов ресурсов, выделяемых на реализацию проекта [31]. В [37] показано, что результатом несбалансированности ресурсов в первую очередь является недостаточная глубина испытаний.

Постановка задачи. Дано: динамика относительного показателя *D(t),* характеризующего выявленные дефекты (например, в виде количества дефектов на 1000 строк кода); динамика затрат ресурсов на выявление дефектов *S(t)*; ограничение на бюджет проекта *S**; ограничение на допустимое число латентных дефектов *D**.

Требуется: оценить сбалансированность показателей *S** и *D**.

Основу решения задачи составляют зависимости *D(t), S(t)* (рисунок 8).

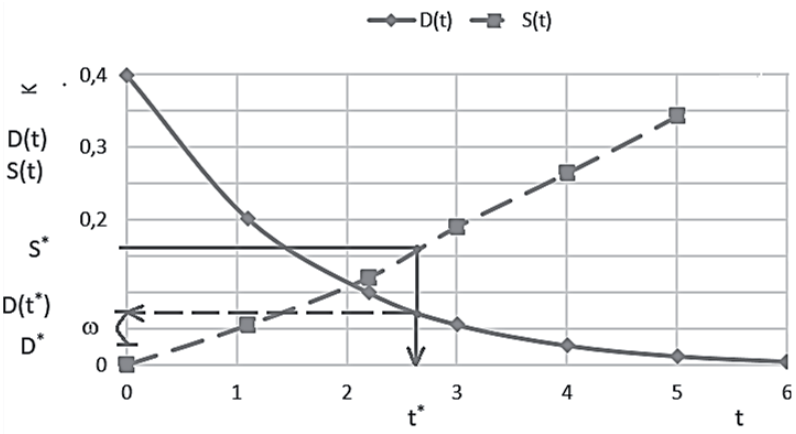

Рисунок 8 - Несбалансированность параметров проекта по показателю количества дефектов

В примере постулированы зависимости *D(t), S(t),* описанные в примере 2. Заданному значению *S** соответствует *t*,* представленное на рисунке 8. Этому значению *t** соответствует показатель *D(t*),* указанный на оси ординат.

Различие $\omega = |D^* - D(t^*)|$ есть характеристика несбалансированности параметров проекта по показателю количества латентных дефектов.

Аналогичным образом можно оценить величину *S(t*),* нужную для обеспечения требуемого значения *D** (рисунок 9).

Следствие несбалансированности нефункциональных требований и объёма выделяемых ресурсов является превышение ограничений на бюджет и время реализации проекта либо несоответствие фактических значений потребительских характеристик программных продуктов желаемым (см. также [24]).

Величина $\gamma = |S^* - S(t^*)|$ есть характеристика несбалансированности по показателю бюджета (рисунок 9). Интегральной характеристикой несбалансированности может служить ин-

декс $I=\sum\alpha_l I_l$, где α_l – весовые коэффициенты, характеризующие значимость ***l***-го показателя ФБ. В качестве индивидуальных индексов приняты $I_1= \omega/ D^*; I_2= \gamma/ S^*$.

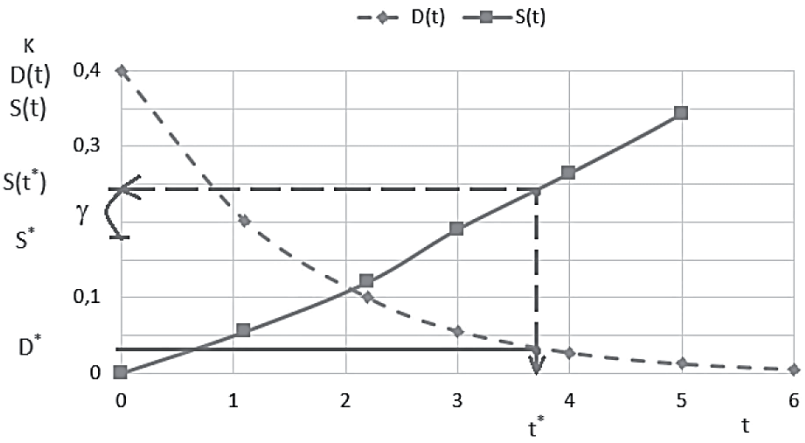

Рисунок 9 - Несбалансированность проекта по показателю бюджета

Рисунок 10 – Структурная модель, соответствующая СА «Эрозия целей»

Описанной задаче может быть поставлен в соответствие СА «Эрозия целей» (рисунок 10). В рамках этого СА несбалансированность желаемых и фактических свойств устраняется за счёт снижения требований к свойствам продукта либо за счёт увеличения объёмов ресурсов.

Заключение

В статье обоснована возможность использования СА как методической основы построения моделей ситуаций, возникающих при решении задач обеспечения ФБ АПК в условиях ограничений на ресурсы.

Дано определение информационной сущности ситуаций, позволяющее создать основу для принятия решений о целесообразности внесения изменений в структуру системы управления СТС.

Предложены концептуальные основы многоаспектного моделирования ситуаций, возникающих при обеспечении ФБ АПК, сочетающие динамические модели параметров, характеризующих ФБ, и структурные модели ситуаций.

Выделены базовые этапы построения системы структурных и динамических моделей ситуаций, возникающих при обеспечении ФБ АПК на разных стадиях их жизненного цикла.

Список источников

[1] *ESA PSS-05-10.* Guide to software verification and validation Prepared by: ESA Board for Software Standardization and Control (BSSC). ESA PSS-05-10 Issue 1 Revision 1. March 1995. 117 p.

[2] ***Виттих В.А.*** Введение в теорию интерсубъективного управления. Самара: Самарский научный центр РАН, 2013. 64 с.

[3] ***Липаев В.В.*** Функциональная безопасность программных средств. Москва: СИНТЕГ, 2004. 348 с.

[4] ***Нагибин С.Я., Пальчун Б.П., Ухлинов Л.М.*** Технологическая безопасность программирования – новая проблема в области создания информационных систем // Информационное общество. 1995. Т.6. С.45-49.

[5] Сопряженное проектирование встраиваемых систем (*Hardware/Software Co-Design*) / С.В. Быковский [и др.]. Санкт-Петербург: Университет ИТМО, 2016. 108 с.

[6] A Driving Assistance System with Hardware Acceleration. – University of Gothenburg, Sweden, 2016.

[7] ***Бородакий Ю.В., Юсупов Р.М., Пальчун Б.П.*** Проблема имитационного моделирования дефектоскопических свойств компьютерной инфосферы // Труды третьей Всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика». Санкт-Петербург, 2007. С.87-32.

[8] ***Рот А.*** Внедрение и развитие Индустрии 4.0. Основы, моделирование и примеры из практики. Москва: Техносфера, 2017. 294 с.

[9] ***Кириллов Н.П.*** Концептуальная модель объекта ситуационного управления функциональным состоянием технических систем // Искусственный интеллект и принятие решений. 2012. Т.4. С.61-75.

[10] ***Мостовой А.Я.*** Управление сложными техническими системами: конструирование программного обеспечения спутников ДЗЗ. Москва: Техносфера, 2016. 352 с.

[11] ***Куликов С.С***. Тестирование программного обеспечения. Базовый курс. Минск: Четыре четверти, 2017. 312 с.

[12] ***Марков А.С.*** Модели оценки и планирования испытаний программных средств по требованиям безопасности информации // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». Специальный выпуск «Технические средства и системы защиты информации». 2011. С.30-103.

[13] ***Cortellessa V., Grassi V.*** A modeling approach to analyze the impact of error propagation on reliability of component-based systems // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2007. P.140-156.

[14] ***Ritu Soni, Ashpinder Preet.*** Cognitive approach to root cause analysis for improving quality of life: a case study for IT Industry. // International journal of informative and futuristic research (Online). Vol. 1. Issue 1, August - September 2013, 8 p.

[15] ***Sunday E.*** Extension and Modification of Anticipatory Failure Determination Approach Based on I-TRIZ. University of Stavanger, Department of Mechanical and Structural Engineering, June 2014, 106 p.

[16] ***Renan Favarão Da Silva, Marco Aurélio De Carvalho.*** Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes, Federal Technological University of Paraná (UTFPR), Curitiba, Brazil, January 2019, 24p. (DOI: 10.1007/978-3-319-78075-7_12)

[17] Error Propagation Analysis of Software Architecture Specifications / D. Nassar [et al.] // Communication. 2006. Vol.1. P.496-501.

[18] ***Lee P.A., Anderson T.*** Fault tolerance, principles and practice // Springer Sci. Bus. Media. 2012. Vol.3. P.320.

[19] ***Verzola I., Lagny A.E., Biswas J.*** A Predictive Approach to Failure Estimation and Identification for Space Systems Operations // Proc. 13th international conference on space operations. – Pasadena, California, USA, 2014.

[20] ***Khater H.A., Mohamed A.B., Kamel S.M.*** A Proposed Technique for Software Development Risks Identification by using FTA Model // World Acad. Sci. Eng. Technol. Int. J. Comput. Inf. Eng. 2013. Vol.7. P.105-111.

[21] ***Pentti H., Atte H.*** Failure Mode and Effects Analysis of Software-Based Automation Systems // STUK-YTO-TR 190. 2002. P.36.

[22] ***Zhu Y.M.*** Failure-modes-based software reading. 2017. P.7-15.

[23] ***Тимофеев А.Н.*** Почему падают ИТ-проекты? // Практика проектирования систем, 2017. С.2-11.

[24] CHAOS Report. The Standish Group International, Inc., 2018, 68 p. https://www.standishgroup.com/news/37.

[25] ***Виттих В.А.*** Неоднородный актор и повседневность как ключевые понятия эвергетики. Самара: Самарский научный центр РАН, 2014. 12 с.

[26] ***Райков А.Н***. Конвергентное управление и поддержка решений. Москва: Издательство ИКАР, 2009. 245 с.

[27] ***Райков А.Н***. Сетевая экспертная поддержка решений // Управление большими системами. 2010. Т.30.1. С.758-772.

[28] ***Сенге П.М.*** Пятая дисциплина. М.: Олимп-Бизнес; 2003. 408 с.

[29] ***Braun W.*** The System Archetypes by Wiiliam Braun. 2002. 25 p.

[30] ***Meadows D.H.*** Thinking in Systems. Chelsea Green Publishing. 2008, 240 p.

[31] ***Hastie S., Wojewoda S.*** Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch. OCT 04, 2015. *https://www.infoq.com/articles/standish-chaos-2015/.*

[32] ***Вентцель Е.С.*** Теория вероятностей. Учебник. -12-е издание. М.: Юстиция; 2018. 658 с.

[33] ***Майерс Г.Дж***. Надежность программного обеспечения. М: Издательство Мир, 1980. 359 с.

[34] ***Бэгьюли Ф.*** Управление проектом. М: Гранд-Фаир; 2002. 208 с.

[35] ***Липаев В.В.*** Надежность и функциональная безопасность комплексов программ реального времени. М: Институт системного программирования РАН; 2013. 207 с.

[36] *ESA PSS 05-11.* Guide to software quality assurance.

[37] ***Макконнелл С***. Сколько стоит программный проект. Санкт-Петербург, 2007. 297 с.

Сведения об авторах

Гвоздев Владимир Ефимович, 1956 г. рождения. Окончил Уфимский авиационный институт им. Орджоникидзе в 1978 г., д.т.н. (2000). Профессор кафедры технической кибернетики Уфимского университета науки и технологий. В списке научных трудов более 370 работ в области прикладного статистического анализа, информационной поддержки управления программными системами, информационной поддержки управления состоянием территориальных систем. AuthorID (РИНЦ): 174520. ORCID 0000-0002-1481-0982. Author ID (Scopus): 7101700484. *wega55@mail.ru*.

Бежаева Оксана Яковлевна, 1977 г. рождения. Окончила Уфимский государственный авиационный технический университет в 2000 г., к.т.н. (2004). Заведующая кафедрой технической кибернетики Уфимского университета науки и технологий. В списке научных трудов более 100 работ в области разработки моделей и программного обеспечения сложных систем, информационной поддержки управления программными проектами и системами. AuthorID (РИНЦ): 271220. ORCIDID 0000-0002-3373-7266. Author ID (Scopus): 57216845244. *obezhaeva@gmail.com*.

Сафина Гульнур Радиковна, 1997 г. рождения. Окончила Уфимский государственный авиационный технический университет в 2022 г., направление «Информатика и вычислительная техника». В списке научных трудов 10 работ в области программно-аппаратных комплексов технических систем. *lafleur300997@gmail.com*.

Поступила в редакцию 17.11.2022, после рецензирования 9.02.2023. Принята к публикации 1.03.2023.

Scientific article DOI: 10.18287/2223-9537-2023-13-1-125-138

Multi-aspect modeling of situation in the functional safety control tasks of hardware and software complexes

© 2023, V.E. Gvozdev, O.Ya. Bezhaeva ✉, G.R. Safina

Ufa University of Science and Technology, Ufa, Russia

Abstract

Functional safety is a latent characteristic of hardware and software complexes (HSC) and is objectively characterized by consumer satisfaction with the HSC behavior. The paper considers an approach to solving project management problems based on the dynamic characteristics analysis of functional safety of conflict situations in the project management system. To analyze situations that arise when managing HSC projects, it is possible to use models known as system archetypes. The information essence of situations and the foundations of multi-aspect modeling are considered. The methodological basis of the research is a combination of dynamic models of parameters that characterize functional safety and structural models, corresponding to conflict situations that arise when ensuring the required level of functional safety. Examples of multi-aspect modeling of situations where manifestations of latent defects act as events are considered. As a result of the research, the information essences of situations are determined, the conceptual foundations of multi-aspect modeling of situations that arise when managing the HSC functional safety are proposed, and the basic stages of building a system of structural and dynamic models of situations at different stages of the HSC life cycle are identified. The results obtained can be used to make decisions about the advisability of making changes to the system structure for ensuring the functional safety of hardware and software complexes..

Key words: *functional safety, hardware and software complex, network-centric management, system archetype, structural models.*

Citation: *Gvozdev VE, Bezhaeva OYa, Safina GR.* Multi-aspect modeling of situation in the functional safety control tasks of hardware and software complexes [In Russian]. *Ontology of designing.* 2023; 13(1): 125-138. DOI: 10.18287/2223-9537-2023-13-1-125-138.

Conflict of interest: The authors declare no conflict of interest.

List of figures and tables

References

[1] *ESA PSS-05-10.* Guide to software verification and validation Prepared by: ESA Board for Software Standardization and Control (BSSC). ESA PSS-05-10 Issue 1 Revision 1. March 1995. 117 p.
[2] ***Vittich VA.*** Introduction to the theory of intersubjective management. [In Russian]. Samara: Samara Scientific Center of the Russian Academy of Sciences, 2013; 64 p.
[3] ***Lipaev VV.*** Functional safety of software tools. [In Russian]. Moscow: SINTEG, 2004; 348 p.
[4] ***Nagibin SYa, Palchun BP, Ukhlinov LM.*** Technological security of programming - a new problem in the field of information systems. [In Russian]. *Information society*, 1995; 6: 45-49.
[5] ***Bykovsky SV.*** Conjugated design of embedded systems (Hardware/Software Co-Design) [In Russian]. Saint Petersburg: ITMO Research Institute, 2011; 125 p.
[6] A Driving Assistance System with Hardware Acceleration. – University of Gothenburg, Sweden, 2016.
[7] ***Borodaki YuV***, ***Yusupov RM, Palchun BP.*** The problem of simulation modeling of flaw detection properties of computer infosphere. [In Russian]. Proceedings of the third All-Russian scientific and practical conference “Simulation. Theory and practice". St. Petersburg, 2007; P.87-32.
[8] ***Roth A.*** Implementation and development of Industry 4.0. Fundamentals, modeling and examples from practice. Moscow: Technosphere, 2017; 294 p.
[9] ***Kirillov NP.*** Conceptual model of the object of situational control of the functional state of technical systems. [In Russian]. Artificial intelligence and decision making. 2012; 4: 61-75.
[10] ***Mostovoy AYa.*** Complex technical systems management: design of remote sensing satellite software. [In Russian]. Moscow: Technosphere. 2016; 352 p.
[11] ***Kulikov SS.*** Software testing. Basic course. [In Russian]. Minsk: Four quarters, 2017; 312 p.
[12] ***Markov AS.*** Models of evaluation and planning of software testing according to information security requirements. [In Russian]. Bulletin Bulletin of Bauman Moscow State Technical University. Special issue "Technical means and information security systems". 2011; P.30-103.
[13] ***Cortellessa V, Grassi V.*** A modeling approach to analyze the impact of error propagation on reliability of component-based systems // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2007. P.140-156.
[14] ***Soni R, Preet A.*** Cognitive approach to root cause analysis for improving quality of life: a case study for IT Industry. // International journal of informative and futuristic research (Online). 2013; 1(1): 8.
[15] ***Sunday E.*** Extension and Modification of Anticipatory Failure Determination Approach Based on I-TRIZ. University of Stavanger, Department of Mechanical and Structural Engineering, June 2014, 106 p.
[16] ***Renan Favarão Da Silva, Marco Aurélio De Carvalho.*** Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes, Federal Technological University of Paraná (UTFPR), Curitiba, Brazil, January 2019, 24p. DOI: 10.1007/978-3-319-78075-7_12.
[17] ***Nassar D.*** Error Propagation Analysis of Software Architecture Specifications. *Communication*. 2006; 1: 496-501.
[18] ***Lee PA***. Fault tolerance, principles and practice / P.A. Lee, T. Anderson // Springer Sci. Bus. Media. 2012; Vol. 3, 320 p.

[19] ***Verzola IA*** Predictive Approach to Failure Estimation and Identification for Space Systems Operations / I. Verzola, A.E. Lagny, J. Biswas // Proc. 13th international conference on space operations. – Pasadena, California, USA, 2014.
[20] ***Khater HA***. A Proposed Technique for Software Development Risks Identification by using FTA Model / H.A. Khater, A.B. Mohamed, S.M. Kamel // World Acad. Sci. Eng. Technol. Int. J. Comput. Inf. Eng. 2013; Vol. 7, P. 105-111.
[21] ***Pentti H, Atte H.*** Failure Mode and Effects Analysis of Software-Based Automation Systems. STUK-YTO-TR 190. 2002; 36p.
[22] ***Zhu YM.*** Failure-modes-based software reading. 2017; P.7-15.
[23] ***Timofeev AN.*** Why IT projects are falling? [In Russian]. Practice of system design, 2017; P. 2-11.
[24] CHAOS Report. The Standish Group International, Inc., 2018, 68 p. - Available: https://www.standishgroup.com/news/37
[25] ***Vittich VA.*** Heterogeneous actor and everyday life as key concepts of evergetics. [In Russian]. Samara: Samara Scientific Center of the Russian Academy of Sciences, 2014; 12p.
[26] ***Raikov AN.*** Convergent management and decision support. [In Russian]. Moscow: ICAR Publishing House, 2009; 245 p.
[27] ***Raikov AN.*** Network expert support of solutions [In Russian]. Management of large systems. 2010; Vol. 30.1, P.758-772p.
[28] ***Senge PM.*** Fifth discipline. [In Russian]. Moscow: Olympus-Business. 2003; 408 p.
[29] ***Braun W.*** The System Archetypes by Wiiliam Braun. 2002; 25p.
[30] ***Meadows DH.*** Thinking in Systems. Chelsea Green Publishing. 2008; 240 p.
[31] ***Hastie S, Wojewoda S.*** Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch. OCT 04, 2015. *https://www.infoq.com/articles/standish-chaos-2015/.*
[32] ***Ventzel ES.*** Theory of Probability. [In Russian]. Textbook. -12th edition. Moscow: Justice, 2018; 658 p.
[33] ***Myers GJ.*** Software reliability. [In Russian]. Moscow: Mir Publishing House, 1980; 359 p.
[34] ***Baguli. F.*** Project Management. [In Russian]. Moscow: Grand-Fair, 2002; 208 p.
[35] ***Lipaev VV.*** Reliability and functional safety of real-time software complexes. [In Russian]. Moscow: Institute of System Programming of the Russian Academy of Sciences, 2013; 207 p.
[36] *ESA PSS 05-11.* Guide to software quality assurance.
[37] ***McConnell S.*** How much does a software project cost? [In Russian]. Peter Publisher; 2007. 296 p.

About the authors

Vladimir Efimovich Gvozdev (b. 1956) graduated from the Ufa Aviation Institute in 1978, D. Sc. Eng. (2000). Professor of the Department of Technical Cybernetics at the Ufa University of Science and Technology (UUST). He is a co- author of about 370 scientific articles and abstracts in the field of applied statistical analysis, information support for managing software systems, information support for managing the state of territorial systems. ORCID 0000-0003-4874-0895.AuthorID (RSCI): 174520. Author ID (Scopus): 7101700484. *wega55@mail.ru*.

Oksana Yakovlevna Bezhaeva (b. 1977) graduated from the Ufa State Aviation Technical University in 2000, PhD. (2004). Head of the Department of Technical Cybernetics at the Ufa University of Science and Technology (UUST). She is a co-author of about 100 scientific articles and abstracts in the field of development of models and software for complex systems, information support for managing software projects and systems. ORCID 0000-0002-3373-7266. AuthorID (RSCI): 271220. Author ID (Scopus): 57216845244. *obezhaeva@gmail.com*. ✉

Gulnur Radikovna Safina (b. 1997) graduated from the Ufa State Aviation Technical University in 2022 in the direction of Informatics and Computer Engineering. She is a co-author of 10 scientific articles and abstracts in the field of software and hardware complexes of technical systems. *lafleur300997@gmail.com.*

Received November 17, 2022. Revised February 9, 2023. Accepted March 1, 2023.